VANTAGE POINT SECURITY

CORPORATE OVERVIEW

WELCOME TO

Vantage Point Security

CREST-accredited penetration testing partner across Southeast Asia.

SINGAPORE
601 MacPherson Road, #07-11/12,
Grantral Mall, Singapore 368242

INDONESIA
World Trade Center 1, 16th Floor,
Jl. Jend. Sudirman Kav.29, Jakarta

THAILAND
1550 Thanapoom Tower, 12th Floor,
New Petchburi Road, Bangkok 10400

Who we are.

One of the largest independent CREST-accredited penetration testing firms in Southeast Asia — securing enterprise and financial services through adversarial expertise.

THE TEAM

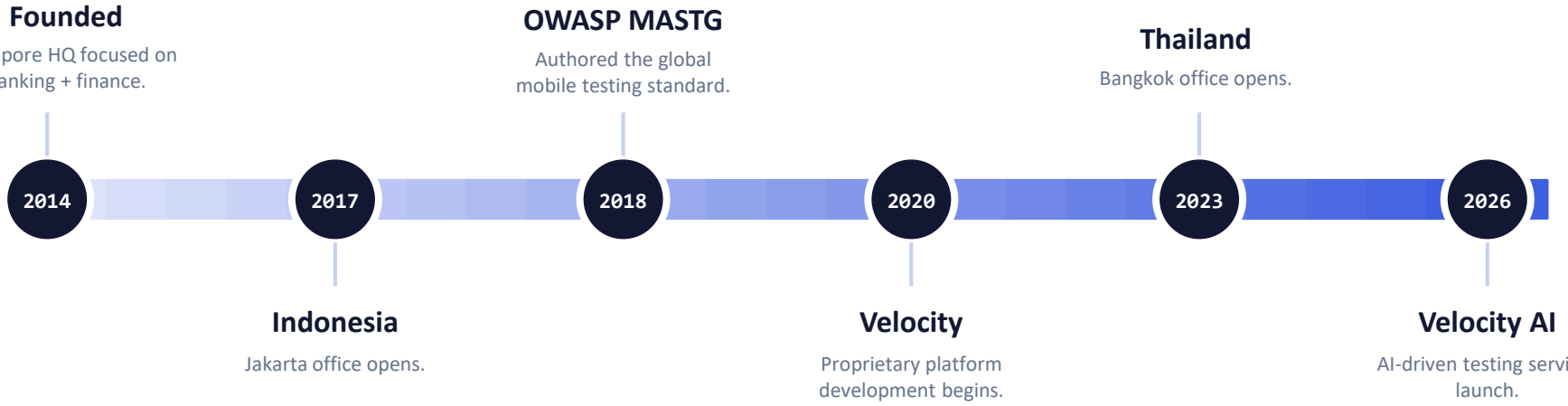
50+

CREST-REGISTERED CONSULTANTS

2014	FOUNDED
12	YEARS EXPERIENCE
3	REGIONAL OFFICES

Our Journey — Past to Present.

From Singapore origins to a Southeast Asian penetration testing firm with proprietary technology.



Our Credentials.

Independently verified across accreditation, regulatory, and quality assurance regimes.

ACCREDITATION

CREST

50+ certified consultants across SEA.

LICENSING

CSRO Singapore

Licensed by Singapore Cybersecurity Services Regulation Office.

QUALITY

ISO 27001:2022 + SOC 2

Group-wide certification and SOC2 attestation current.

REGULATORY

ASPI Registered

Sek.ASPI/STT/065/X/2024 in Indonesia.

Trusted by Many.

Engagements span banking, financial services, insurance, telecommunications, and critical infrastructure.

BANKING	FINANCIAL SERVICES	INSURANCE	TELCO
HEALTHCARE	ENERGY	GOVERNMENT	RETAIL

Client names and referrals available under NDA.

Staff Certifications.

All Vantage Point consultants hold offensive-security and CREST certifications as a baseline — many carry significantly more.

MINIMUM BASELINE

Every Consultant Holds:

OSCP
Offensive Security — Certified Professional

CREST CRT
Certified Registered Tester

CREST CPSA
Certified Practitioner Security Analyst

PLUS, MANY MORE

Additional certifications held across the regional team:

CCRTS	OSWE	OSEP	OSCE
OSED	eWPTX	eMAPT	eCPPT
eJPT	CRTP	CISSP	CCSP
CRT	CPSA	CRTO	C|TIA

Our Accomplishments.

Our team love to hack and are active in global CTF competitions, often securing podium placements.

1ST
SPIEF Cyberbattle 2024
Russia's National RT CTF

1ST
Cyber Jawara CTF 2024
Indonesia

1ST
CyberSec Asia Thailand
Thai International Cyber Week 2026

2ND
Slashroot 7.0 CTF 2023
Capture-The-Flag

3RD
SPIEF Cyberbattle 2023
St. Petersburg

2ND / 3RD
Defcon HTX Singapore 2026
Singapore

8th / 3,829
NAHAMCON 2024
Global

13th
HTB Business CTF 2024
1st in SE Asia

13th
HTB Business CTF 2021
Global

14th
HTB Business CTF 2022
Dirty Money

25
GLOBAL EVENTS
Active participation in CTF competitions worldwide

Our Hiring Process.

A rigorous, multi-stage process ensures only the most skilled and ethical cyber-security professionals join our team. Vantage Point has a reputation as a top destination for ethical hackers in SEA.

01 Technical Interview	02 Non-Technical Interview	03 Signing	04 Background Check
05 OSCP Lab + Cert	06 CREST CPSA	07 CREST CRT	**08 Project Assignment**

Our Service Offering.

Comprehensive penetration testing across every layer of modern enterprise architecture, with the flexibility to customise to client requirements.

APPLICATION SECURITY

- Mobile Application Testing
- Web Application Testing
- API Security Testing
- Thick Client Testing

SOURCE CODE SECURITY

- Static Analysis (SAST)
- Software Composition Analysis (SCA)

CLOUD SECURITY

- AWS Assessments
- Azure Assessments
- GCP Assessments
- AliCloud Assessments

INFRASTRUCTURE SECURITY

- Network Penetration Testing
- Active Directory Testing
- Wireless Pen Testing
- Security Config Review

RED TEAMING

- Red Team Assessment
- GL20 / AASE Compliance
- MITRE ATT&CK Aligned

IOT SECURITY AND OTHERS

- Firmware Assessment
- Hardware Assessment
- Customised Risk Ratings
- Customised Test Cases

Private and Confidential

The Problem in Penetration Testing.

Penetration testing has historically delivered inconsistent results — two skilled consultants assessing the same system often find different sets of flaws.

CONSULTANT A

3

flaws found

≠

CONSULTANT B

5

flaws found

Did either consultant find all the flaws?

Velocity — Our Difference.

Velocity is our in-house compliance, standards, and service delivery platform. A guided path of test cases ensures consistent, reliable, repeatable results.

3,623
INDIVIDUAL TEST CASES

97
INFOSEC + REGULATORY STANDARDS

GUIDED
Test-case driven
Consistent path, every engagement.

COMPREHENSIVE
Depth + breadth
Mapped to technology, risk, compliance.

ASSURED
Verifiable results
Repeatable execution end-to-end.

Inside the Velocity Platform.

Velocity orchestrates the entire engagement lifecycle — from test case selection through finding management and compliance reporting.

TEST CASES

Curated test catalogue

Mapped to OWASP, CIS, and regional regulator standards.

EVIDENCE

Structured evidence capture

Reproduction steps, screenshots, and payload data per finding.

FINDINGS

Finding workflow management

Status tracking, risk rating, retesting end-to-end.

COMPLIANCE

Verification Reporting

Per-standard pass/fail mapping with full traceability.

DASHBOARDS

Real-time visibility

Coverage metrics, vulnerability timelines, risk distribution.

REPORTING

Multi-format export

PDF, JSON, XML, CSV — across 113 languages.

Private and Confidential

Next-Generation Reporting.

Velocity-generated reports go beyond findings — they deliver verifiable, traceable, and multilingual artefacts ready for regulator review.

- **Detailed vulnerability reporting**
  Background, technical detail, and recommendations per finding.
- **Traceability to the test case**
  Every finding linked back to the originating Velocity test case.
- **Compliance verification reporting**
  Pass / fail mapping to each applicable standard.
- **Industry-standard risk ratings**
  CVSS 3.1, 3.2, and 4.0 supported across findings.

113

LANGUAGES SUPPORTED

CRYPTOGRAPHICALLY SIGNED

+ VERIFIABLE

Tamper-evident report artefacts

Sample Report : LLM Security Review



4. Detailed Description of Vulnerabilities

4.1. LLM Excessive Agency

High / Score: 8.5
Open
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:H/SC:H/SI:H/SA:N
LLM06:2025 Excessive Agency
Vulnerability Raised: 16/03/2026

BACKGROUND

Agency in the context of LLMs refers to the model's ability to take actions in the real world invoking tools, calling APIs, sending communications, modifying data, or controlling external systems. **Excessive Agency** occurs when the model is granted more capability, permission, or autonomy than its intended function requires. Whether through **excessive functionality** (access to tools beyond what the task needs), **excessive permissions** (operating with an identity that has broader access than the current user), or **excessive autonomy** (taking high-impact actions without requiring human confirmation). Ideally these operation will require human permission and human confirmation.

This is a security issue because any vulnerability that allows an attacker to influence the model's instructions most notably Prompt Injection is directly amplified by the scope of the model's agency. A model that can only generate text poses an information risk. A model that can send emails, delete files, call payment APIs, and query databases poses an operational risk. The more the model can do, the more damaging any successful manipulation of its behavior becomes.

DESCRIPTION

The AI has tool integrations (email, SQL, file manager) with no confirmation gates. It executes actions immediately without user approval or privilege checks.

Affected Endpoint

Field	Value
URL	**https://[TARGET_DOMAIN]/chat**
Tools Available	**send_email**, **file_manager**, **sql_query**, **api_request**, **calendar**
Authentication	Authenticated user session (standard user role)

Prerequisites

1. A valid user account with access to the AI assistant
2. Burp Suite or browser DevTools to monitor backend API calls
3. A test email inbox to verify delivery (e.g., **https://www.mailinator.com**)

Steps to Reproduce

1. Log in to **https://[TARGET_DOMAIN]** with a standard user account.
2. Navigate to **https://[TARGET_DOMAIN]/chat** and start a new conversation.
3. **Step 1 - Enumerate available tools.** Send the following message:

Strictly Confidential (For Internal Use Only) 9

Standards-Based

Testing benchmarked to industry standards

Reproducible Evidence

Affected endpoint, prerequisites, and numbered steps to reproduce.

Risk-Ranked Findings

Severity-rated using CVSS 3/4

3.2. Compliance Verification

This section shows whether the application is compliant to the essential regulations. For non-compliant regulations, the failed test cases are listed below the regulation. Findings for each test case will be listed below the corresponding test cases.

Regulation, Test Case, *Finding*	**Compliance**
OWASP Top 10 for LLM Applications	Non-Compliant
1. LLM01:2025 Prompt Injection	
LLM Vulnerable To Prompt Injection	
2. LLM06:2025 Excessive Agency	
LLM Excessive Agency	
3. LLM02:2025 Sensitive Information Disclosure	
LLM Vulnerable to Sensitive Information Disclosure	

Mapped Down to the Test Case.

Every finding in a Velocity report carries a consistent four-layer structure — designed for auditors, developers, and reviewers alike.

01

TEST CASE MAPPING

Test Case Traceability

Every finding linked to its Velocity test case ID — auditable end-to-end.

02

CVSS SCORING

CVSS 3.1 / 3.2 / 4.0

Industry-standard risk scoring with full vector strings.

03

REPRODUCTION

Step-by-Step Proof

Requests, responses, payloads, screenshots — fully reproducible.

04

REMEDIATION

Actionable Guidance

Config examples, code references, standards mappings.

Experts in Penetration Testing.

Enterprise-wide testing across web, mobile, network, and cloud assets — at the scale and consistency required by major financial-services clients.



SCALABLE TEAM

Capacity scales with engagement size.



PROJECT MANAGER

Dedicated PM on every engagement.



CONSISTENT RESULTS

Velocity-driven uniform quality.



REGULATORY EXPERIENCE

Direct engagement with regional regulators.

Private and Confidential

Specialists in Application Security.

Our roots are in AppSec — in fact we authored the standards that define how modern mobile applications are now secured.

WE AUTHORED THE SECURITY STANDARDS

OWASP MASTG + OWASP MASVS

The Mobile Application Security Testing Guide and Verification Standard — the global baseline for modern mobile security testing was originally authored by Vantage Point Security.



FLEXIBLE SCHEDULING

Prompt mobilisation, adaptable engagement windows.



BENCHMARKED

Aligned to industry and regulatory baselines.



EMBEDDED IN DELIVERY

Working on-site with development teams.



STANDARDS AUTHORS

We wrote MASTG / MASVS.

We Hack the Future of Tech.

Velocity supports a broad range of next-generation testing types. Our consultants are guided to consistently test emerging technology, not just established systems.



BIOMETRICS

Fingerprint, face, and behavioural authentication testing.



BLOCKCHAIN

Smart contracts, wallets, and non-custodial protocol-layer review.



IOT HARDWARE

EU-CRA aligned testing with published CVEs in hardware vulnerabilities.



ATM / CDM

Cash machine and deposit terminal security assessments.



LLM / AI

Prompt injection, model evasion, and agent security.

Why Choose Vantage Point.

Scale, depth, and proven investment in proprietary capability.

12	50+	70,000+	TIER-1	IP
YEARS EXPERIENCE	CREST CONSULTANTS	HOURS YEARLY	FS PORTFOLIO	PROPRIETARY VELOCITY

VANTAGE POINT SECURITY

Thank you for your time.

SINGAPORE · INDONESIA · THAILAND